Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Information Technology

Unit 11: Cyber Security and Incident Management Part B

Window for supervised period:
Monday 30 April 2018 – Monday 21 May 2018
Supervised hours: 4 hours

Paper Reference
20158K

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this task is 37.

Turn over ▶

P57173A

1/1/1/1/1/1

P 5 7 1 7 3 A

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for candidate use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 25 May 2018.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your teacher/tutor.

Set Task Brief

Black Country Training and Assessment

Black Country Training and Assessment (BCTAA) offers vocational-based training and assessment services for small and medium-sized businesses.

Some training is routine, such as running food safety or IT skills courses. It uses a database of freelance trainers and assessors to meet client requirements.

BCTAA also develops bespoke training and assessment for specialised skills, such as the maintenance of unusual machinery or working with a unique production process. Bespoke training requires collaboration with the client and often includes handling highly confidential information, such as trade secrets.

BCTAA has recently moved to offices on the 19th floor of Edexcelsior House (EH) near the city centre. EH has mixed commercial and office usage. The 18th floor is leased by a recruitment agency, the 20th floor houses a restaurant and coffee bar with bar-cafe on the roof garden above. The ground floor contains several small retail units. Other floors contain a gymnasium, an art gallery and meeting rooms. The rest is office space, is occupied by a variety of different companies.

Most of the public areas are open outside of normal office hours and the restaurant and bar are popular in the evening.

A plan of the new BCTAA offices, is shown in **Figure 1**. The lifts, stairwells, WCs and associated areas are open to the public.

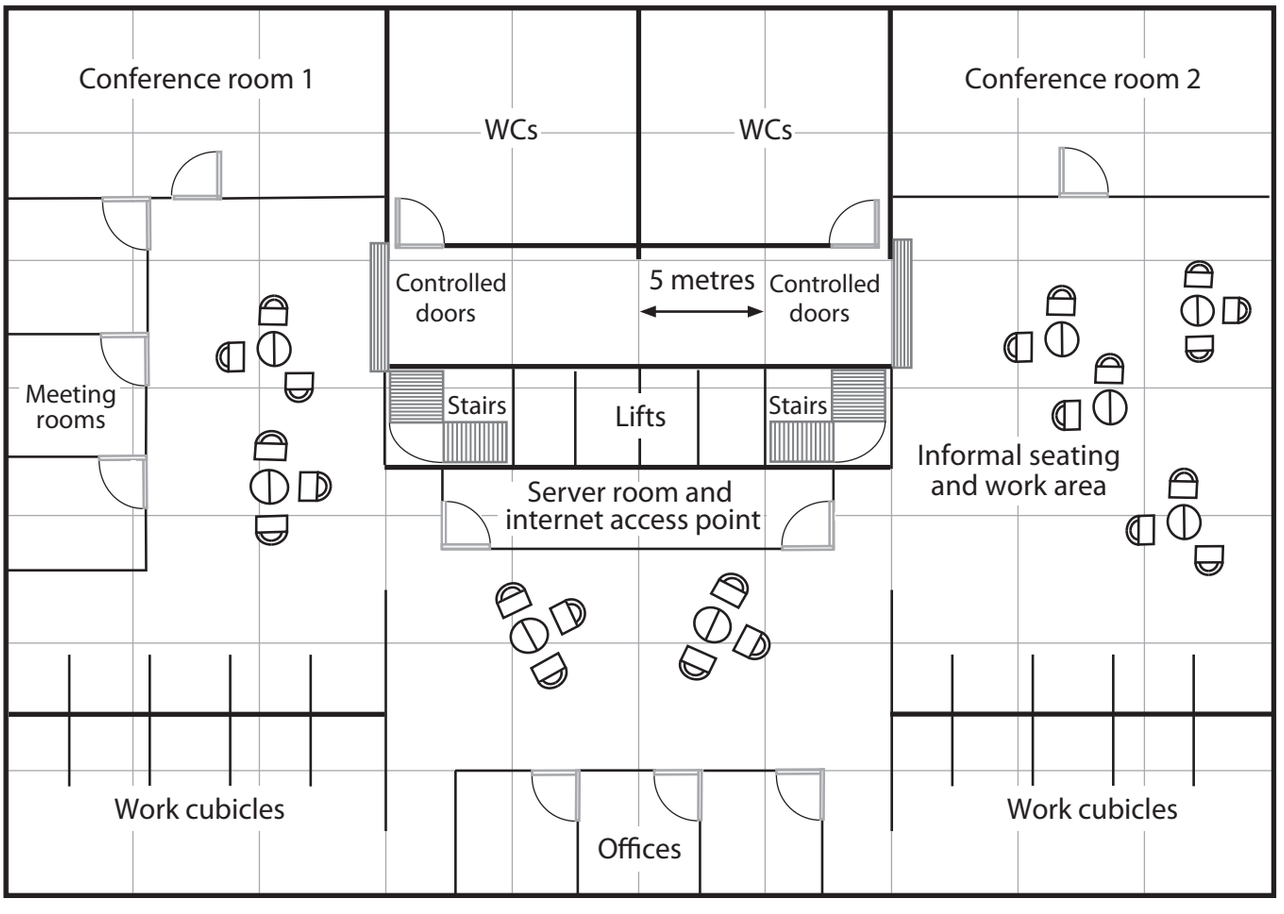


Figure 1

Client brief

You advised Baljinder Singh of BCTAA on security matters for the move to the new location. Now, a few weeks later, he has called you in to review the investigation of a cyber security incident.

A short while ago, over the course of a Bank Holiday weekend (31st March - 2nd April 2018), a number of small items went missing from the BCTAA premises. These items included USB sticks, wireless mice and keyboards, a company mobile phone and a laptop computer.

Baljinder investigated the losses and also liaised with EH management company and the police. The results of the investigation were inconclusive, but he believes that EH was targeted by an organised gang that has since moved on to other locations.

Evidence items from the security incident at BCTAA

Evidence items include:

1) Baljinder's account
2) summary of a meeting with the EH management company
3) door access control logs
4) network diagram
5) laptop tracking report
6) cyber security document – incident management policy.

1. Baljinder's account

It all happened over the Bank Holiday weekend. Most people had left by Friday lunchtime and the place was empty by 14:00. The missing items had been used for meetings in the informal seating and work area. They really should have been put away, but the phone and laptop had been left plugged in and charging on one of the tables. We didn't notice anything wrong until the Tuesday afternoon, when the laptop had been booked for another meeting and we couldn't find it. We had a search for it and that was when we realised that other items were missing as well. The final list is:

- Surface Pro 3 laptop
- Samsung Edge S5 phone
- 3 x USB memory sticks, various sizes and makes
- 3 x wireless mouse and 2 x wireless keyboards, various makes.

The problem is that although we're sure that the laptop and phone went missing over the Bank Holiday weekend, we can't be certain when the other items disappeared.

We notified the police and talked to the EH management company. The police gave us an incident number for insurance purposes, but without evidence of forced entry there wasn't much they could do. The laptop was four years old and the phone three, so we didn't bother making an insurance claim.

We did notify the phone company to get the phone blocked and also started tracking the laptop via 'Find My Device'. **(See evidence item 5)**.

The EH management company said that there had been a few incidents over the Bank Holiday weekend. I met with them on Wednesday to discuss things. **(See evidence item 2)**. Fortunately the working files on the laptop had been copied to the file server at the end of the meeting. The original files would still have been there, but the team were

working on assessing the safe operation of fire extinguishers, so there is nothing really secret there.

2. Summary of a meeting with the Edexcelsior House management company

Baljinder's notes from a meeting with senior management on the Wednesday after the incident.

People present; representatives from the EH management company, restaurant and bar, ground floor shops, the recruitment agency from the 18th floor.

(a) Assurances about cleaners, maintenance workers, etc. All cleaning, maintenance, security and similar staff are employed directly by EH. Wages and conditions are deliberately better than those for similar jobs in the area. This reduces staff turnover and encourages loyalty. There have been very few dismissals for dishonesty and none this year.

(b) A number of pickpocketing and opportunity thefts had been reported on Friday evening in the shops, bar and restaurant areas. These areas were extremely busy and CCTV footage was inconclusive. Extra security staff were visibly deployed in those areas on Saturday. Thefts returned to their normal, low background level for the rest of the Bank Holiday weekend.

(c) BCTAA and the recruitment agency both reported thefts, without evidence of forced entry, happening over the Bank Holiday weekend, with no evidence of forced entry. The recruitment agency lost some small electronics items from its reception area.

(d) The shops reported problems with customers having phantom charges applied to some contactless payment cards. The cards affected are issued by the EH management company to handle loyalty points and are valid for all goods and services in the building. Phantom charges have occasionally happened in the past due to system errors. The system was checked and no errors were found in the card readers or software. Phantom charges from the three days of the Bank Holiday weekend have been re-credited as a goodwill gesture.

3. Annotated door access control log

All doors are controlled through a networked system, using near field communication /proximity cards, similar to those used for contactless payment systems. The EH management company supplies cards, a card programming device and logging and control software as part of the leasing arrangement. The doors can also be unlocked from the inside by pushing a button.

The cards hold a 10 digit number. When someone approaches a controlled door they just need to pass their card within 10 cm of the reader. The number is then read and compared with those stored for that reader.

For example a 10 digit number, (0123456789), has the format:

01 – floor number.
23 – business number
456789 – staff/personal number

BCTAA is on the 19th floor and has a business number of 63. All BCTAA cards start with 1963.

The software allows access to be restricted by date and/or time.

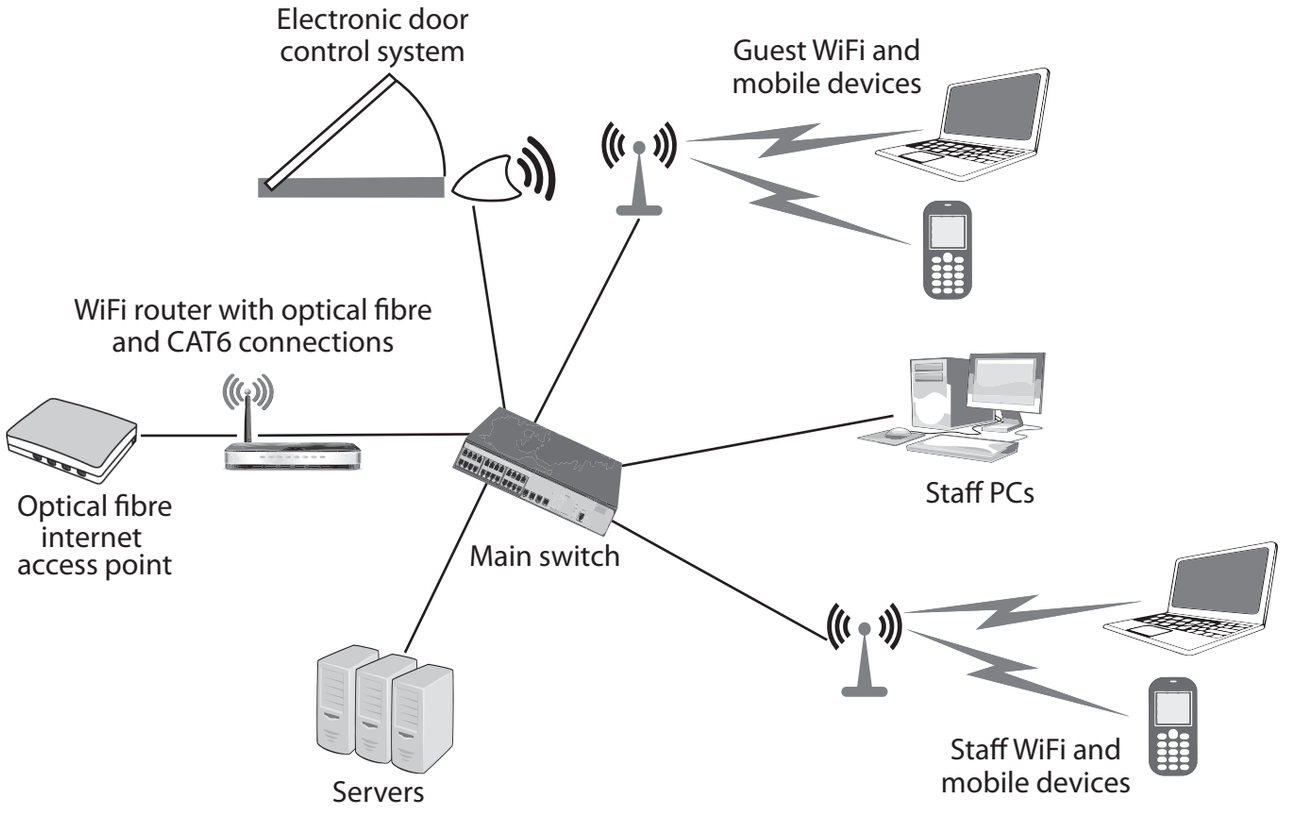
The EH management company uses cards starting with 99. These allow 24/7 access for cleaning, maintenance and security purposes. Access via 99 cards is logged on the BCTAA system and also sent via a network link to the management company where it is checked against scheduled access. Some unscheduled access is allowed, e.g. for security staff, but it produces an alert on the system.

BTCAA 19th floor log from 13:00 Friday 30th March to 08:00 Tuesday 3rd April.

	Card number	Date–time	In/Out	Notes
1	19630 00026	03301342	Out	Last group leaving after work. The person with card 26 opened the doors, let everyone out, checked the offices were empty and left at 1342 on 30th March.
2	99110 02126	03301824	In	Scheduled cleaning staff
3	99110 02291	03301824	In	Scheduled cleaning staff
4	99110 02126	03301919	Out	Scheduled cleaning staff
5	99110 02291	03301919	Out	Scheduled cleaning staff
6	99220 01185	03302218	In	Security check
7	99220 01185	03302220	Out	Security check
8	99220 01193	03310622	In	Security check
9	99220 01193	03310624	Out	Security check

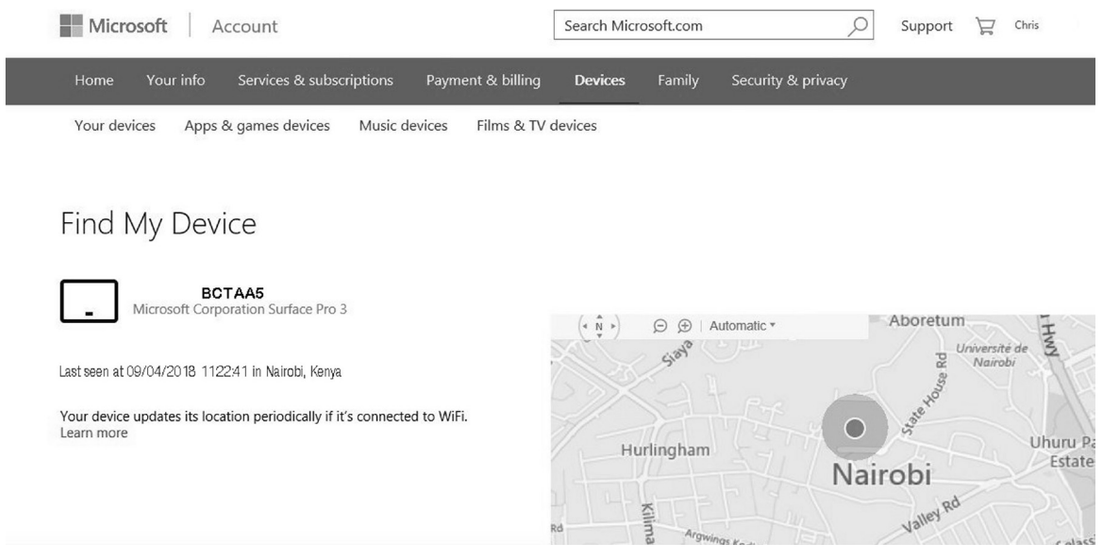
10	99220 01177	03311412	In	Security check
11	99220 01177	03311413	Out	Security check
12	99220 01185	03312220	In	Security check
13	99220 01185	03312221	Out	Security check
14	19630 00035	03312331	X	Correct card but time limited so no access. Card holder says they were at a BCTAA party on the 20th floor and is certain they didn't try to gain access.
15	18420 00775	03312331	X	Correct card for floor 18. Card holder denies using it but admits to being at the party that evening and cannot remember if he used the card or not.
16	19630 00029	03312332	X	Correct card but time limited so no access. Card holder says they were at a BCTAA party on the 20th floor and is certain they didn't try to gain access.
17	19630 00010	03312332	In	Correct card. Card holder is BCTAA senior management and has 24/7 access. Card holder says they were at a BCTAA party on the 20th floor and is certain they didn't try to gain access.
18	99220 01193	04011211	In	Security check
19	99220 01193	04011213	Out	Security check
20	99220 01177	04012346	In	Security check
21	99220 01177	04012348	Out	Security check
22	99220 01185	04021220	In	Security check
23	99220 01185	04021221	Out	Security check
24	99220 01137	04022333	In	Security check
25	99220 01137	04022335	Out	Security check
26	19630 00086	04030755	In	First BCTAA staff member enters offices on 3rd April.

4. Network diagram



5. Laptop tracking report

After activating the Windows10, Find My Device system on the 3rd April, a single notification was received a week later. No further reports were received.



6. Cyber security documentation - incident management policy

Incident management team

The team shall consist of:

- the network manager or the deputy (team leader)
- the senior BCTAA manager present at the time of the incident
- the BCTAA public relations officer.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the team leader or their deputy. If both are unavailable the report should be made to the senior BCTAA manager present at the time. The incident may be reported verbally but this must be followed by a written or digital account. It is the responsibility of the team leader to maintain documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of data
- unauthorised access to company IT systems
- infection of IT systems with malware.

Incident response procedures

(a) Theft of IT equipment

- Once a theft is discovered, collect as much information as possible (location and type of equipment, serial numbers, when it was last seen, etc.).
- The team leader must ascertain if the item has actually been stolen (or if it has simply been moved or mislaid). This task may be delegated for minor items that do not pose a security risk.
- If the item is confirmed as stolen the team leader must inform the senior manager and public relations members of the team, who will determine if the police need to be involved and who will run any internal enquiry .
- Where a stolen item may have contained confidential material, data theft must be assumed and the procedures given in b) followed in addition to a).
- The team must prepare reports on the theft for BCTAA management, police, insurers, and other interested parties.
- The team should review the incident and implement procedures to prevent future losses.

(b) Theft of data

- Any loss or theft of data (actual or suspected) must be reported at once to the team leader.
- The team leader must investigate the loss and identify, as far as possible, what data has been lost or stolen and when the incident occurred.
- In the event that the data contains or may contain personal identifiable information (PII) or other confidential materials, the senior manager and public relations officer will determine if a breach of data protection legislation may have occurred and who will run any internal enquiry.
- Having identified what has been lost or stolen, the team must retrieve backups and restore the data as soon as possible.
- The team must prepare reports on the theft for BCTAA management, police and other interested parties.
- The team should review the incident and implement procedures to prevent future losses.

(c) Infection of company IT systems with malware

- Any member of BCTAA staff who suspects that any IT system has been compromised by malware must report the incident at once to the team leader.
- The infected system should be isolated as soon as possible.
- The team leader will investigate the infection and take appropriate measures to resolve the infection and restore the system.
- In the event of a severe infection, which disrupts the day-to-day business of BCTAA or which may cause a breach of data protection legislation, the team leader must inform the senior manager and public relations officer. They will determine if a reportable breach of data protection legislation has occurred and will run any internal enquiry.
- The team should review the incident and implement procedures to prevent future infections.

(d) Unauthorised access to BCTAA systems

- Any member of BCTAA staff who suspects that there has been unauthorised access to any BCTAA IT system must report it at once to the team leader, providing as much detail as possible (which system, how access was obtained).
- The team leader will investigate the incident and identify how the unauthorised access was obtained.
- The team leader will take whatever action is required to prevent future occurrences (change passwords, etc.).
- Where the unauthorised access may have allowed confidential information to be seen, data theft should be assumed and the procedures given in b) followed in addition to d).
- The team should review the incident and implement procedures to prevent future unauthorised access.

Part B Set Task

You must complete ALL activities in the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You advised Baljinder Singh of BCTAA on security matters for the move to the new location. Now, a few weeks later, he has called you in to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at BCTAA.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–5 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–6 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS

BLANK PAGE

BLANK PAGE